IMPLEMENTASI GROUP BLIND DIGITAL SIGNATURE DALAM SISTEM E-VOTING PEMILIHAN KEPALA DAERAH

Muhammad Yusuf [1)], **Taufiqur Rohman**[2)]
[1,2)] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Trunojoyo Madura
Jl. Raya Telang PO BOX 2 Kamal, Bangkalan, 69162 Madura Telp (031)-3011146
e-mail : muhammadyusuf@trunojoyol.ac.id, taufiq_104@yahoo.co.id

Abstrak
Pemilihan kepala daerah di Indonesia masih bersifat konvensional sehingga kurang efektif dan masih banyak kekurangan dan kesalahan akibat human error terutama dalam hal perhitungan suara. dibutuhkan sistem pemungutan suara yang dapat meminimalisir human error tersebut. E-voting merupakan salah satu solusi pengganti system voting konvensional, dalam e-voting peran manusia tergantikan dengan komputer terutama dam hal perhitungan suara, sehingga kesalahan dalam perhitungan suara dapat diminimalisir. Untuk menjaga kerahasiaan sistem e-voting ini menggunakan kriptografi yang berupa group blind digital signature yang merupakan variasi dari tanda tangan dijital yang dibangun berdasarkan algoritma RSA. Melalui enkripsi data, sistem ini mengamankan data kandidat yang telah dipilih oleh pemilih, sehingga kerahasiaan pilihan tetap terjaga. dalam penelitian sistem e-voting yang dilaksanakan ini, group blind digital signature digunakan pada saat pengiriman data dari instansi yang ada dalam proses pemilihan kepala daerah untuk otentifikasi data yang dikirimkan.

***Kata Kunci** : group blind digital signature, e-voting, pemilihan kepala daerah.*

1. PENDAHULUAN

Dalam kehidupan masyarakat yang mengutamakan demokrasi, voting atau pemungutan suara merupakan metode yang sangat penting dalam menetukan keputusan, voting digunakan untuk menghimpun aspirasi dari seluruh elemen masyarakat, dan kemudian menemukan jalan keluar yang dianggap paling baik untuk menyelesaikan permasalahan. Pemilihan umum merupakan bagian pada suatu proses demokrasi, pelaksanaan pemilihan umum kepala daerah atau yang lazim disebut Pemilu Kada yang dilakasanakan di Indonesia masih bersifat konvensional, dalam pelaksanaan voting secara konvensional banyak kekurangan dan terjadi kesalahan yang disebabkan *human error*, kekurangan yang paling banyak dijumpai adalah lamanya proses perhitungan suara yang juga berpotensi terjadinya kesalahan dalam proses perhtungan hasil suara, kelemahan lain yang ada dalam sistem voting konvensional yakni pemilih berpotensi melakukan kesalahan dam memberikan tanda dapa pilihanya. Permasalahan-permasalahan tersebut yang membuat keabsahan voting terkadang diragukan.

Untuk mengantisipasi kesalahan tersebut di atas dibutuhakan sebuah sistem voting yang melibatkan sumber daya manusia yang sedikit, sehingga human error dapat berkurang, dengan tetap mengutamakan asas pemilu yakni LUBER (langsung umum bebas rahasia) dan JURDIL (jujur dan adil). Voting secara elektronik atau yang lazim disebut e-voting merupakan salah satu solusi untuk permasalahan tersebut. Sistem voting elektronik yang dibutuhkan adalah sistem dengan kemampuan menjaga data dari manipulasi pihak yang berkepentingan tertentu. Dengan penggunaan sistem e-voting diharapkan kesalahan-kesalahan yang sering terjadi bisa berkurang, diharapkan juga perhitungan suara hasil voting dapat lebih cepat selesai sehingga segera dapat diketahui hasil dari voting tersebut.

Masalah keamanan dan kerahasian data menjadi hal yang mutlak diperhatikan dalam pelaksanaan e-voting, untuk memenuhi hal tersebut dibutuhkan suatu teknik agar bisa menjaga keamanan dan kerahasian data, teknik tersebut adalah kriptografi, kriptografi merupakan Teknik untuk mengacak suatu pesan agar tidak dapat diketahui maknanya Prinsip dasar kriptografi adalah menyembunyikan informasi sedemikian rupa sehingga orang yang berhak saja yang dapat mengetahui isi dari informasi yang tersembunyi tersebut.

Algoritma kunci publik merupakan salah satu teknik kriptografi yang dapat melakukan enkripsi dan dekripsi data serta penandaan digital (*digital signature*). Penggunaan algoritma kunci publik pada sistem e-voting untuk melakukan enkripsi pada data untuk menjaga keamanan dan kerahasiaan data. Pada sistem e-voting ini menggunakan algoritma RSA untuk keamanan data pemilih dan teknik *group blind digital signature* untuk keamanan ditribusi data.

2. TINJAUAN PUSTAKA

2.1. E-VOTING

Pengertian dari electronic voting (e-voting) secara umum adalah penggunaan teknologi komputer pada pelaksanaan voting. Pilihan teknologi yang digunakan dalam implementasi dari e-voting sangat bervariasi, seperti penggunaan smart card untuk autentikasi pemilih, penggunaan internet sebagai sistem pemungutan suara, penggunaan touch screen sebagai pengganti kartu suara, dan masih banyak variasi teknologi yang digunakan.
Pada e-voting terdapat beberapa skema yang harus dipenuhi, skema tersebut bertujuan untuk keamanan e-voting termasuk untuk menjamin privasi atau kerahasiaan pemilih. Skema e-voting adalah sebagia berikut;
Eligibility: hanya pemilih yang terdaftar yang dapat melakukan pemilihan. Unreusability: setiap pemilih hanya bisa memberikan satu kali pilihan. Anonymity: pilihan pemilih dirahasiakan. Accuracy: pilihan tidak bisa diubah atau dihapus selama atau setelah pemilihan dan juga tidak bisa ditambahkan setelah pemilihan ditutup. Fairness: perhitungan suara sebelum pemilihan ditutup tidak bisa dilakukan. Vote and Go: pemilih hanya dapat melakukan pemilihan saja. Public Verifiability: setiap orang dapat melakukan pengecekan pada berjalannya proses pemilihan

2.2. KRIPTOGRAFI

Kriptografi merupakan Teknik untuk mengacak suatu pesan agar tidak dapat diketahui maknanya Prinsip dasar kriptografi adalah menyembunyikan informasi sedemikian rupa sehingga orang yang berhak saja yang dapat mengetahui isi dari informasi yang tersembunyi tersebut.
Tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu: kerahasiaan, integritas data, autentikasi, dan non-repudiasi.

2.3. ALGORITMA RSA

Salah satu algoritma kunci publik yang paling polpuler dalam kriptografi adalah algoritma RSA, algoritma RSA dibuat oleh 3 orang peneliti dari *Massachussets Institute of Technology* pada tahun 1976, yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. Kemanan algoritma RSA terletak pada sulitnya memfaktoran bilangan-bilangan yang besar menjadi bilangan prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan tersebut belum ditemukan maka selama itu pula keamanaan RSA masih terjaga.
Algoritma RSA didasarkan pada teorema euler yang menyatakan bahwa :

$a^{\phi(n)} \equiv 1 \pmod{n}$. (1)

Pada RSA, algoritma pembangkit kunci dinyatakan sebagai berikut:
1. Pilih dua bilangan prima sembarang,p dan q.
2. Hitung n=p . q (sebaiknya p ≠ q).
3. Hitung Φ(n)= *(p - 1) (q - 1).*
4. Pilih kunci Publik e yang relative prima terhadap Φ*(n).*
5. Bangkitkan kunci prifat dengan persamaan berikut:

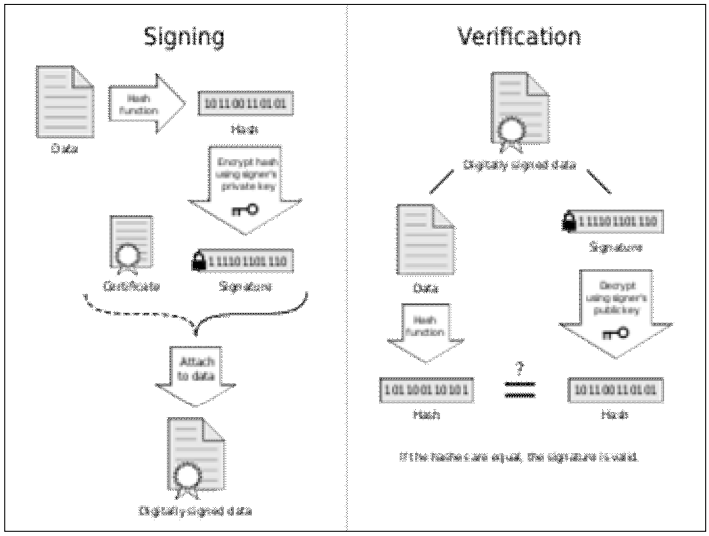
$$d = \frac{1 + k\Phi(n)}{e} \quad (2)$$

Sedangkan untuk enkripsi dan dekripsi secara berturut-turut digunakan rumus sebagai berikut
$E_e(m)=m^e \bmod n$. (3)
$D_d(c)=c^d \bmod n$. (4)

2.4. DIGITAL SIGNATURE

Tanda tangan dijital (*Digital Signature*) merupakan tanda tangan untuk data dijital. Tanda tangan dijital bukanlah tulisan tanda tangan yang di-digitisasi (*di-scan*), melainkan suatu nilai kriptografis yang bergantung pada isi pesan dan kunci.
Selain digunakan untuk menjamin integritas data, tanda tangan dijital juga dapat digunakan untuk membuktikan asal pesan (keabsahan pengirim), dan nirpenyangkalan.
Menandatangani pesan dapat dilakukan dengan salah satu dari dua cara, yaitu tanda tanga dengan enkripsi pesan dan tanda tangan digital dengan fungsi hash.
Pemberian tanda tangan dengan mengenkripsi pesan dapat dilakuakn dengan algoritma kunci publik, salah satu algoritma kunci publik yang banyak digunakan adalah algoritma RSA.
Adapun langkah pemberian tanda tangan digital dengan algoritma RSA adalah sebagai berikut :
1.Pengirim menghitung nilai hash dari pesan M yang akan dikirim, misalkan nilai hash dari pesan M adalah h.
2.Pengirim mengenkripsi h dengan kunci privatnya menggunakan persamaan enkripsi RSA, yaitu:
$S = h^{SK} \bmod n$ (5)
3.Pengirim mengirim M + S ke penerima

Sedangkan proses verifikasi tanda tangan adalah menggunakan persamaan dekripsi pesan pada RSA.



Gambar 1. Visualisasi pemberian tanda tangan digital.

2.5. GROUP DIGITAL SIGNATURE

Group digital signature merupakan metode yang dapat membuat sesorang menjadi wakil suatau kelompok untuk menandatangani dokumen. Pada skema group digital signature, anggota dari suatu kelompok dapat melakukan tanda tangan dijital pada suatu dokumen atas nama seluruh anggota kelompok. Tanda tangan tersebut dapat diverifikasi dengan menggunakan kunci publik kelompok (*group public key*).

Skema group digital signature terdapat lima prosedur sebagai berikut:

1. Setup, dalam proses ini dilakukan pembangkitan kunci publik kelompok dan sebuah kunci rahasia administrasi yang dilakukan oleh ketuakelompok.
2. Join, pembangiktan kunci individu(private key) untuk setiap anggota kelompok dilakukan oleh ketua kelompok.
3. Sign, proses penanda tanganan oleh anggota kelompok menggunakan kunci private yang telah diberikan kepada anggota yang bersangkutan.
4. Verify, proses verifikasi tanda tangan yang ada pada dokumen yang diterima dari pengirim pesan, verifikasi dilakukan menggunakan kunci publik yang dimiliki kelompok pengirim pesan. proses ini dilakukan oleh penerima pesan.
5. Open, proses ini ditujukan untuk mengetahui anggota yang telah melakukan tanda tangan, proses ini hanya bisa dilakukan oleh ketua kelompok yang megirim pesan beserta tanda tangan dengan menggunakan kunci private yang dimiliki kelompok yang bersangkutan.

Pada group digital signature pembangkit kunci untuk individu yang ada dalam kelompok (group) adalah sebagai berikut: [6]

$n_n=P_aP_b$ (6)

$d=e^{-1} \bmod \Phi(n_n)$ (7)

Dimana n_n merupakan modulo untuk individu ke-n, d merupakan kunci privte dari individu dan e merupakan kunci publik dari individu

2.6. GROUP BLIND DIGITAL SIGNATURE

Group digital signature pertama kali dikemukakan oleh Lysyanskaya dan Ramzan. Group blind digital signature mengkombinasikan properti dari grup signature dan blind signature.

Group blind digital signature merupakan gabungan dari blind digital signature dan group digital signature. sehingga dapat dikatakan group blind digital signature adalah group digital signature yang diberikan pada pesan yang telah di samarkan (blinding).

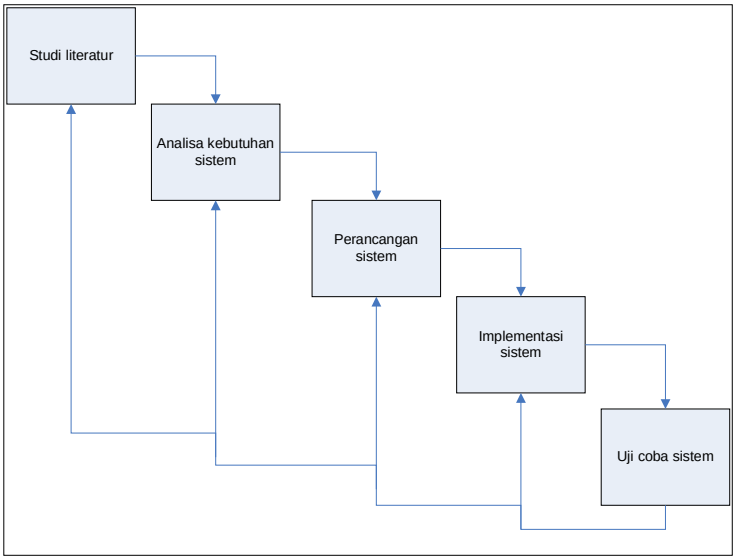
Kebutuhan keamanan dari Group Blind Digital Signature sangat mirip dengan yang dimiliki Group Digital Signature. Penambahan yang ada kita membutuhkan properti penyamaran dalam pesan. Berikut kebutuhan-kebutuhan dari group blind digital signature:

•*Blindness of Signature*: pemberi tanda tangan harus tidak dapat melihat isi dari pesan yang ia beri tanda tangan, walaupun penerima dapat memverifikasi bahwa tanda tangan tersebut valid.

•*Soundness and Completeness*: tanda tangan yang valid akan selalu benar saat diverifikasi, dan tanda tangan yang tidak valid akan selalu tidak dapat melewati proses verifikasi.
•*Unforgeable*: Hanya anggota grup yang dapat membuat tanda tangan kelomok yang valid.
•*Signer ambiguous*: Apabila diberikan pesan beserta tanda tangannya, identitas dari individu pemberi tanda tangan tidak dapat ditentukan tanpa kunci rahasia manager.
•*Unlinkability*: Antara satu anggota dengan anggota yang lain berbeda.
•*No Framing*: Tidak ada anggota kelompok termasuk ketua kelompok yang dapat membuat tanda tangan untuk pihak yang tidak berpartisipasi dalam kelompok.
•*Unforgeable tracing verification*: ketua kelompok tidak dapat salah menyatakan bahwa individu tersebutlah yang memberi tanda tangan padahal sebenarnya tidak.
•*Undeniable Signer Identity*: Ketua dari kelompok selalu dapat member tahu siapa yang memberika tanda tangan yang valid
•*Coalition Resistance*: Hanya ketua kelompok yang dapat membuat melakukan setup group signature yang valid.

Seperti halnya syarat keamanan pada group digital signature, protokol atau prosedur pada group blind digital signature pun sama persis seperti protokol pada group digital signature. Protokol-protokol tersebut yaitu: setup, join, sign, verify, dan open.
Beberapa kelebihan dari group blind digital signature yang juga merupakan bagian dari digital signature antara lain adalah dalam hal autentifikasi data yang dikirim, karena pemberian tandatangan hanya dapat dilakukan dengan menggunakan kunci privat yang dimiliki anggota kelompok, maka pada saat ferivikasi tanda tangan yang ada dalam pesan valid maka pihak penerima dapat memastikan bahwa data dikirim dari kelompok yang dimaksud.
Telah dilakukan enkripsi terhadap pesan data yang dikirim yang membuat pesan tidak dapat terbaca oleh pihak lain selain penerima dan pengirim pesan. hal ini yang dapat menjaga integritas data yang dikirim.
Dalam penggunaan group blind digital signature seseorang yang telah melakukan tandatangan tidak dapat menyangkal bahwasanya bukan dirinya yang melakukan tandantangan terhadap pesan yang dikirim, karena dalam group blind digital signature data seseorang yang melakukan tandatangan dapat dibuktikan dengan menggunakan kuci privat yang dimiliki oleh meneger atau ketua kelompok.

3. METODE PENELITIAN



Gambar 2. sistematika penelitian

3.1.Studi literatur
Pada tahap ini dilakukan pembelajaran dari buku, jurnal, tugas akhir ataupun paper yang nantinya bisa menjadi acuan dalam membangun sistem yang akan dibuat. Buku atau paper yang dibutuhkan dalam studi leiteratur ini antara lain adalah buku atau paper yang membahas tentang elektronik voting, kriptografi, penelitian tentang e-voting dan sumber-sumber lain yang membahas semua tentang elektronik voting.
Hasil yang diperoleh setelah melakukan study litertur yakni analisis dan desain system selanjutnya.

3.2.Analisa kebutuhan sistem
Setelah melakukan studi literatur langkah selanjutnya yakni analisa dan identifikasi system yang ada saat ini, dalam hal ini yang perlu dikerjakan adalah menganalisa keperluan apa saja yang nantinya digunakan dalam membangun sistem.

3.3.Perancangan sistem
Pada tahap ini akan dirancang system yang sesuai dengan analisa sebelumnya, pemodelan system

3.4.Implementasi dan Sistem
Tahap selanjutnya adalah implementasi sistem, dalam tahap ini adalah tahap pembangunan sistem

3.5.Ujicoba Sistem
Dalam tahap ini dilkukan pengujian system dengan cara melakukan simulasi pelaksanaan e-voting yang telah dibangun.

4. HASIL DAN PEMBAHASAN

Keamanan sistem yang diterapkan pada sistem e-voting ini meliputi:
1.Penerapan Captcha
Penerapan captcha ini digunakan untuk mencegah pembobolan pada halaman login yang dapat dilakukan oleh program komputer seperti metode brute force yang mencoba menebak id dan password secara acak dengan segala kemungkinan kombinasi karakter, tetapi metode tersebut tidak bisa membaca captcha. Karena tidak ada program komputer yang bisa membaca susunan teks seperti manusia.

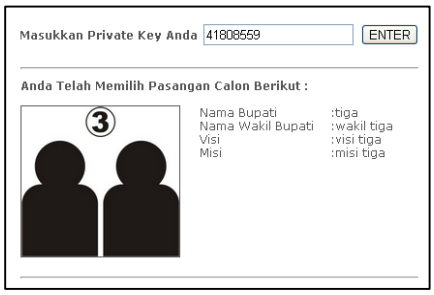
2.Penggunaan Session
Session digunakan pada setiap halaman untuk mengecek apakah setiap pengguna yang mengakses halaman itu mempunyai hak atau tidak, jika pengguna tidak berhak maka sistem tidak akan mengizinkan pengunjung untuk mengakses halaman tersebut. Untuk halaman pemilih hanya dapat dilihat oleh pemilih yang sudah login ke sistem begitu juga untuk halaman administrator. Setiap session yang dibuat akan selalu dicocokkan dengan basis data.

3.Penerapan Algoritma RSA
Penerapan algoritme ini digunakan untuk mengenkripsi data pilihan pemilih dan juga data yang akan didistribusikan ke tempat lain yang sudah disepakati. Penerapan algoritma ini juga digunakan dalam menyisipkan tandatangan digital (digital signature) yang dapat dilakukan oleh petugas yang mewakili kelompok (group)
Algoritme RSA dapat membuat kunci publik, kunci privat, dan modulo secara otomatis ketika pemilih telah melakukan pemilihan, yang selanjutnya private keynya akan ditampilkan kepada pemilih untuk disimpan. Sedangkan untuk private key dan public key yang digunakan untuk signature sudah di atur oleh ketua kelompok dan didistribusikan kepada anggota kelompok.

Implementasi sistem e-voting ini berbasis web yang dijalankan dalam web broser, sistem yang dibangun digunakan oleh pemilih dan admin dalam hal ini panitia penyelnggara voting.
Setelah pemilih berhasi login maka sistem akan menampilkan pasangan kandidat yang dapat dipilih oleh pemilih.
Gambar 3 berikut ini adalah Form untuk memilih kandidat di sistem e-voting.

Gambar 3. **F**orm untuk memilih kandidat

Sedangkan Gambar 4 berikut ini adalah Form untuk meilhat pilihan pada sistem E-Voting ini.



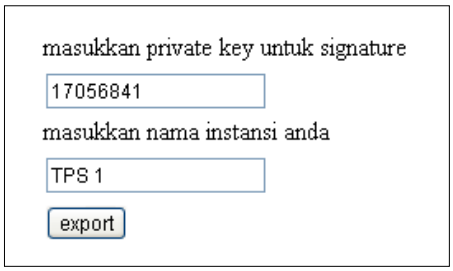
Gambar 4. Form untuk melihat pilihan

Pada Gambar 5 berikut ini adalah Pilihan Pemilih yang telah di enkripsi.

id_pemilih	pilihan
35.26.010.001.000913	15184947 8356241 21226214 10983152 30008993 176098...
35.26.010.001.000911	36157160 29848711 4581352 38570058 7223598 3915475...

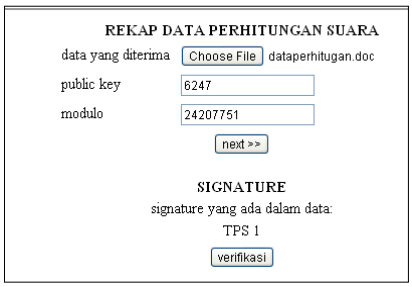
Gambar 5. pilihan pemilih yang di enkripsi

Pilihan pemilih dienkripsi dan disimpan dalam basis data. Sistem akan menampilkan *private key* pemilih, pemilih menggunakan *private key* yang dimiliki untuk melihat pilihanya kembali setelah proses pemilihan selesai maka pemilihan ditutup dan panitia penyelenggara mengirimkan hasil perolehan suara yang berada di TPS kepada Panitia penyelenggara melalui jaringan komputer yang telah ditentukan, untuk menjaga keamanan data maka data tersebut dienkripsi dan di veri tandatangan digital untuk proses otentifikasi. Gambar 6 berikut ini adalah Pengisian Digital Signature.



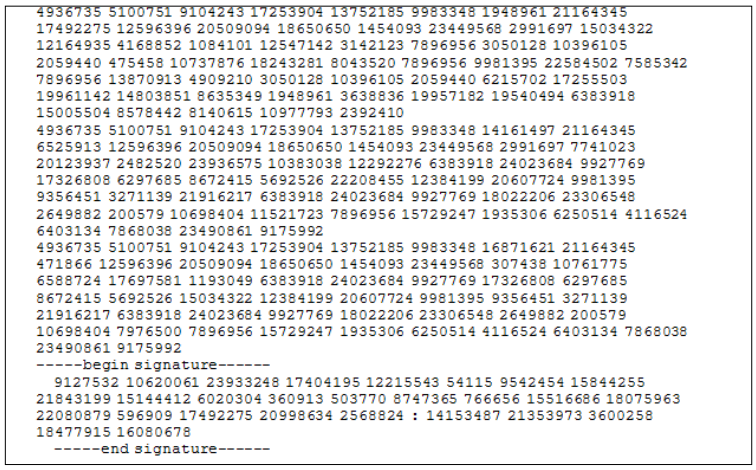
Gambar 6. Pengisian Digital Signature

Sedangkan Gambar 7 ini adalah proses Verifikasi Signature yang ada dalam sistem E-Voting ini.



Gambar 7. verifikasi signature

Panitia penyelenggara memberikan tandatangan digital dengan cara memasukkan *prívate key* yang telah diberikan sebelumnya, kemudian data dikirimkan dan diterima oleh pihak yang dituju, kemudian pihak penerima memeriksa *signature* yang ada dalam data yang diterima dengan memasukkan *public key* yang dimiliki oleh instansi (*group*) yang mengirimkan data (*pesan*). Gambar 8 berikut ini adalah kumpulan data yang telah dienkripsi dan disertai Group Blind Digital Signature.



Gambar 8. Data yang telah dienkripsi dan disertai Group Digital Signature

5. KESIMPULAN

Berdasarkan percobaan yang telah dilakukan terhadap sistem maka dapat disimpulkan beberapa hal sebagai berikut:

1.Sistem telah mewakili sistem voting konfensional.

2.Sistem hanya bisa dijalankan dengan alur yang telah ditentukan.

3.Penggunaan *group blind digital signature* pada sistem e-voting yang dibangun menghasilkan data yang di enkripsi (*blind*) yang ditambahkan tandatangan digital (*digital signature*) yang dilakukan oleh perwakilan kelompok *(group)* yang berguna untuk menjaga keamanan dan integritas serta otentifikasi data pada saat pengiriman data.

DAFTAR PUSTAKA

Arifin, Z., Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman. *Jurnal Informatika Mulawarman.* 4: 3.2009

Hopkins DW, Collins TW, Wierenga SW. ***group signature generation system using multiple primes*:** United States Patent. 2006

Isnaini,MF., 2009, *Analisis dan Implementasi E-voting System pada Pemilihan Kepala Daerah.* Bogor:Institut Pertanian Bogor.

Munir, R. 2006, *Kriptografi.* Informatika. Bandung.

Ramzan ZA. *Group Blind Digital Signatures: Theory and Applications***.** Massachusetts Institute Of Technology. Cambridge: 1999.

Ridwan.. **Studi mengenai group blind digital signature**. Institut Teknologi Bandung: Program Studi Teknik Informatika. 2006.